

Appl. No. 09/905,113

Amdt. Dated: May 26, 2005

Reply to Office Action of: December 7, 2004

Amendments to the Claims

This listing of claims will replace all prior versions and listings of claims in the application:

Listing of claims:

Claim 1 (currently amended): A method of verifying data integrity between at least two correspondents in a ~~public-key~~ cryptographic scheme, at least one of said at least two correspondents having a main processor and a secure module, said secure module being independent of said main processor's control, said method comprising the steps of:
assembling data on at least one of said at least two correspondents;
displaying said data under control ~~[[by]]~~ of said main processor to produce a first output;
forwarding said data to said secure module and displaying said data from said secure module to
produce a second output;
~~comparing to permit comparison of~~ said first output and second output; and
instructing said secure module to generate a signature on said data upon a favorable comparison of said first output and said second output; ~~[[and]]~~
whereby said favorable comparison indicates data integrity such that said at least one of said correspondents signs said data.

Claim 2 (original): The method of claim 1, wherein said at least one of said at least two correspondents is a personalized device.

Claim 3 (original): The method of claim 2, wherein said personalized device is a mobile phone.

Claim 4 (original): The method of claim 2, wherein said personalized device is a personal digital assistant.

Claim 5 (currently amended): The ~~system method~~ of claim 1, wherein said ~~favourable~~ favorable comparison is characterized in that said first output and said second output are logically related

Appl. No. 09/905,113

Amdt. Dated: May 26, 2005

Reply to Office Action of: December 7, 2004

to one another.

Claim 6 (currently amended): The ~~system~~ method of claim 5, wherein said logical relationship is such that said first output and said second output are identical.

Claim 7 (currently amended): The ~~system~~ method of claim 1, wherein said step of displaying said data message includes displaying a portion of said data message.

Claim 8 (currently amended): The ~~system~~ method of claim 7, wherein said ~~favourable~~ favorable comparison is characterized in that a portion of said first output and a portion of said second output are logically related to one another.

Claim 9 (currently amended): The ~~system~~ method of claim 8, wherein said logical relationship is such that said portion of said first output is identical to said portion of said second output.

Claim 10 (currently amended): A method of establishing a ~~seeure~~ trusted communication path for data between a personalized device and ~~[[an]]~~ a user of said device in a ~~[[PKI]]~~ cryptographic scheme, said device having a main processor and a secure module independently operative of said main processor, said method comprising the steps of:
providing an interface between said device and said user, said interface having an input device and an output device for providing a means for interaction between said user and device, said input device and output device controllable by said main processor;
providing a ~~seeure~~ trusted communication path between said secure module and a secure input device and a secure output device coupled thereto, said ~~seeure~~ trusted path logically isolated from any other communication path;
assembling data at said input device and said secure input device and forwarding said data to said secure module over said trusted communication path; and
displaying said data on said output device and said secure output device, to permit comparison of
~~comparing~~ said data displayed on said output device and said secure output device;
whereby said user of said personalized device can determine said integrity of said data based on

Appl. No. 09/905,113

Amdt. Dated: May 26, 2005

Reply to Office Action of: December 7, 2004

said comparison.

Claim 11 (original): The method of claim 10, wherein said user actuates said secure input device based only on said output of said secure output device.

Claim 12 (currently amended): A method for verifying the integrity of a data message between a correspondent and a personalized device in a communication system, each correspondent adapted to receive and transmit data messages, said method comprising the steps of:
containing a secret key in [[said]] a secure module, said secure module adapted to be removably coupled to said personalized device and communicatively coupled thereto; and
controlling access to said personalized device based on a comparison of data from said secure module and data from a main processor of said personalized device, said main processor independently operable of said secure module.

BEST AVAILABLE COPY